McLaren Health Care says data breach impacted 2.2 million people

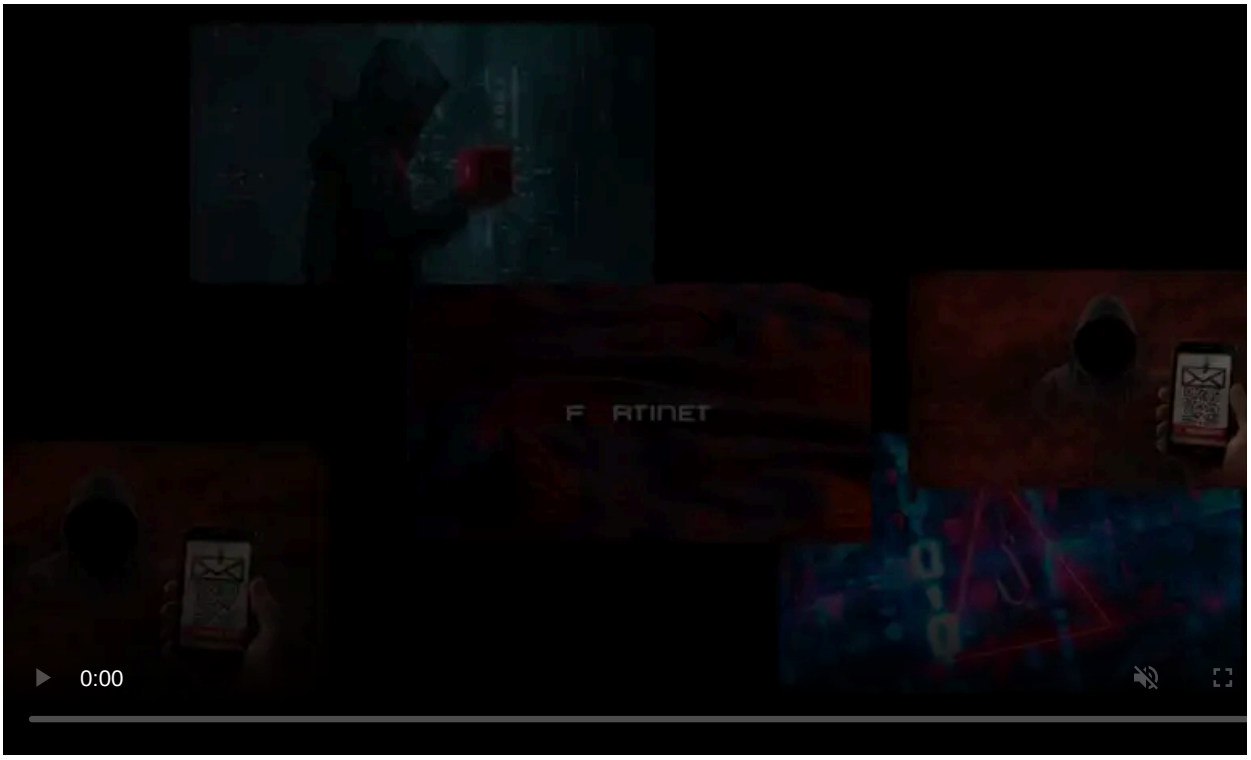
By Bill Toulas

Published: 2023-11-10 · Archived: 2026-04-05 21:07:27 UTC

McLaren Health Care (McLaren) is notifying nearly 2.2 million people of a data breach that occurred between late July and August this year, exposing sensitive personal information.

McLaren is a non-profit healthcare system with an annual revenue of $6.6 billion. It encompasses an extensive network across Michigan that includes 14 hospitals with a total bed capacity of 2,624 and is supported by a team of 490 physicians.

The organization boasts a substantial workforce, with a 28,000 full-time staff. Additionally, it maintains contractual relationships with 113,000 providers, extending its reach into Indiana.


F RTINET
0:00

McLaren published a statement on its website about the intrusion and also notified U.S. authorities. The organization also alerted impacted individuals of the incident.

Per the provided information, McLaren identified a security breach on August 22, 2023. Subsequent investigations, conducted with the assistance of external cybersecurity experts, revealed that the breach had compromised its systems since July 28, 2023.

Evidence shows that on August 31 an unauthorized threat actor had accessed data and the following data types were confirmed to have been exposed by October 10:

- Full name
- Social Security number (SSN)
- Health insurance information
- Date of birth
- Billing or claims information
- Diagnosis
- Physician information
- Medical record number
- Medicare/Medicaid information
- Prescription/medication information
- Diagnostic results and treatment information

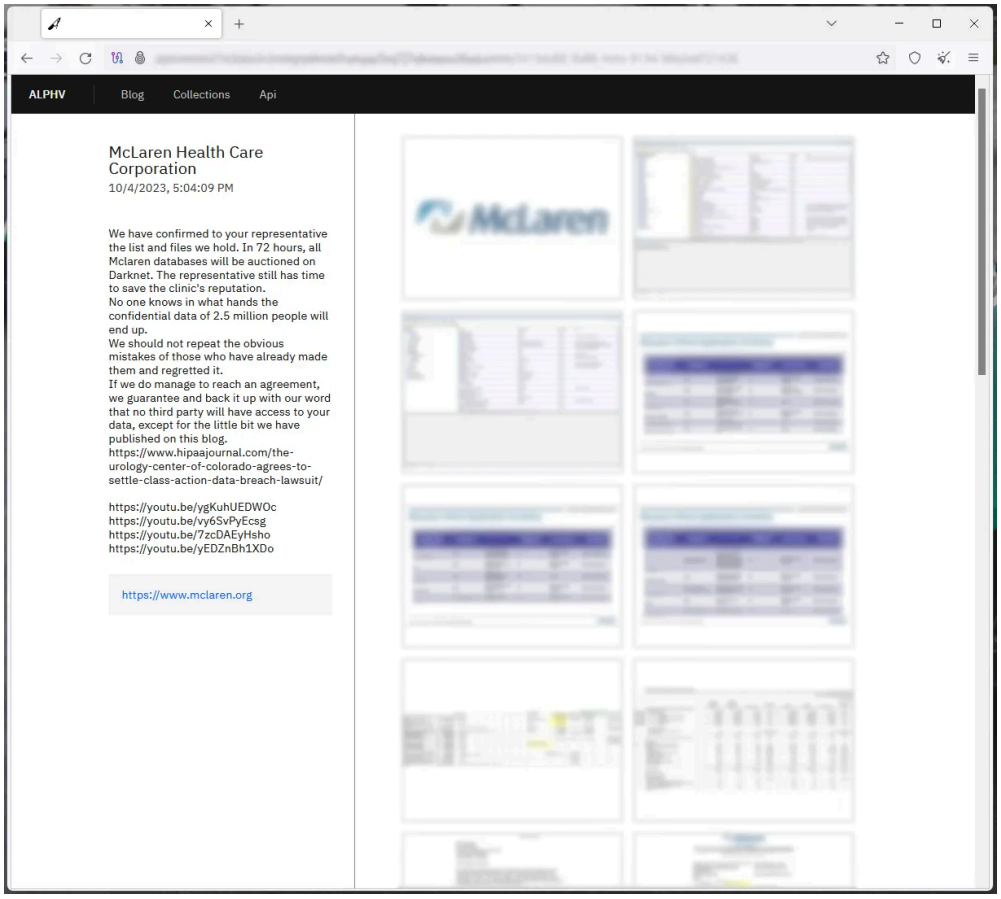
The specific types of data exposed differ for each individual, depending on the information they shared with the organization and the services they received.

All impacted individuals will receive to the email address they provided to McLaren a notification with instructions on enrolling to identity protection services for 12 months.

McLaren says it currently holds no evidence that cybercriminals abused the exposed data but urges impacted individuals to be cautious with unsolicited communications and keep a close eye on their bank account activity.

“While there is currently no evidence that your information has been misused, we recommend that you remain vigilant, monitor and review all of your financial and account statements and explanations of benefits, and report any unusual activity to the institution of record and to law enforcement.” - McLaren

Although the organization does not disclose many details about the cyberattack, it is worth mentioning that the ALPHV/BlackCat ransomware group took responsibility for an attack on McLaren's network on October 4.



McLaren claimed by BlackCat ransomware in October *(BleepingComputer)*

The threat actors published samples of the data they allegedly stole from McLaren and threatened to auction the entire data set that they claim to impact 2.5 million people.
